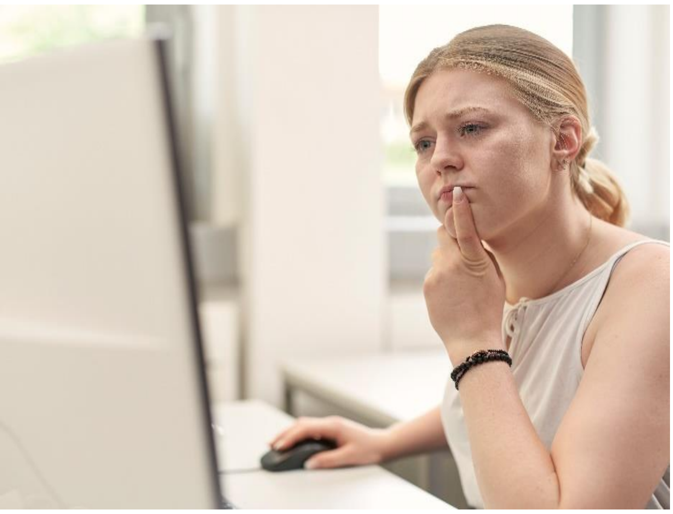
Press Release

No. 048 | afr | June 09, 2020

Phishing Campaigns and Their Pitfalls

Researchers of Karlsruhe Institute of Technology and Bochum University Analyze the Effect of Feigned Phishing Mails to Sensitize Staff



Open or not? The senders of phishing mails often pretend to be known service providers or colleagues. (Photo: Amadeus Bramsiepe, KIT)

Fake emails are used most frequently by cybercriminals to obtain access to confidential data by fraud or to introduce malware. Some companies try to test and supposedly enhance the resistance of their staff to such attacks with the help of phishing campaigns. In this case, the staff is deliberately sent a simulated phishing mail. The report published by scientists of Karlsruhe Institute of Technology (KIT) and Ruhr Universität Bochum highlights phishing campaigns under the aspects of security, law, and the human factor.

Fake emails, the senders of which pretend to be known service providers, colleagues, or superiors appear to be credible. Their target is to make innocent addressees click a link in order to access accounts and passwords or to introduce malware. A single staff member trusting a phishing attack is sufficient to cause serious damage. To test how employees react to phishing mails, some companies and institutions use phishing campaigns of external service providers. With the knowledge of the management, fake phishing mails are sent to the staff members.

Monika Landgraf
Chief Press Officer,
Head of Corp. Communications

Kaiserstraße 12
76131 Karlsruhe, Germany
Phone: +49 721 608-21105
Email: presse@kit.edu

Press contact:

Carola Mensch
Press Officer
Phone: +49 721 608-21170
Email: carola.mensch@kit.edu

Additional material:

To the report: https://publikationen.bibliothek.kit.edu/1000119662
(in German)

“The campaigns are aimed at deliberately deceiving employees in order to protect them against real dangers and to create a problem awareness, but often it is not clear what is legally, technically, and ethically acceptable,” the scientists say. These aspects are analyzed by Professors Melanie Volkamer, Head of the research group SECUSO – Security, Usability, and Society at KIT, and Franziska Boehm from KIT’s Center for Applied Legal Studies, in cooperation with M. Angela Sasse, Professor for Human-Centred Security at the Horst Görtz Institute for IT Security, Bochum. Their research report that is freely accessible online describes various forms and targets of phishing campaigns and associated aspects of IT and information security, employee and data protection, trust culture, and self-efficacy of employees. The report analyzes the validity and pitfalls of such campaigns and offers information for IT and information security officers among others.

“Phishing campaigns are associated with a number of security problems and strongly influence the culture of trust and error handling at a company. In addition, several legal aspects have to be considered,” Boehm says. Apart from her professorship at KIT, she also heads the Department for Intellectual Property Rights in Distributed Information Infrastructures (IGR) of FIZ Karlsruhe – Leibniz Institute for Information Infrastructure. “Starting a campaign without informing the staff in advance is unfair and does not enhance trust in the management,” says Sasse, who conducts research at the Cluster of Excellence of Cyber Security in the Age of Large-scale Adversaries, CASA for short. She graduated in labor psychology and computer science. When people are informed that they have been taken in by phishing mails, this adversely affects their self-efficacy: “The staff members notice that they have no control of this situation and react with resignation. They do no longer try to detect phishing mails,” the authors point out.

“When the employees know, however, that the campaign has started, they may be curious and click a mail in the assumption that nothing can happen, because the mail is faked. Still, real phishing mails continue to circulate, which reduces the protection level,” says Volkamer, who conducts research at the Competence Center for Applied Security Technology Karlsruhe (KASTEL), one of three competence centers for cyber security in Germany. The problem is aggravated, she says, when an employee notices that he or she has clicked a dangerous link and does not dare to report it. Prior to starting a phishing campaign, it is therefore important to establish an obligation to report IT security incidents at a company, the computer scientist emphasizes.

In case of an announced campaign, employees are expected to question far more mails and to be overcautious. This may increase the time and performance pressure, which also has a negative impact on trust in the management. “Security mostly is felt to be annoying and troublesome anyway. In our opinion, the big problem of phishing campaigns is that the negative connotation of this matter is increased, because in the end, it is the management that attacks its staff,” Sasse says. The authors recommend companies that wish to increase their IT security to invest the time and money in an improvement of technical security measures. Only then is it reasonable to train the staff as to the phishing mails that may reach them in spite of the latest security software and operation system and how these mails can be detected.

Original publication:

Melanie Volkamer (KIT, SECUSO, KASTEL), M. Angela Sasse (RUB, CASA), Franziska Boehm (KIT, FIZ): Phishing-Kampagne zur Mitarbeiter-Awareness. Analyse aus verschiedenen Blickwinkeln: Security, Recht und Faktor Mensch (phishing campaigns for staff awareness. Analysis from various perspectives: Security, law, and the human factor). https://publikationen.bibliothek.kit.edu/1000119662 (in German)

Being “The Research University in the Helmholtz Association,“ KIT creates and imparts knowledge for the society and the environment. It is the objective to make significant contributions to the global challenges in the fields of energy, mobility and information. For this, about 9,300 employees cooperate in a broad range of disciplines in natural sciences, engineering sciences, economics, and the humanities and social sciences. KIT prepares its 24,400 students for responsible tasks in society, industry, and science by offering research-based study programs. Innovation efforts at KIT build a bridge between important scientific findings and their application for the benefit of society, economic prosperity, and the preservation of our natural basis of life. KIT is one of the German universities of excellence.

This press release is available on the internet at http://www.sek.kit.edu/english/press_office.php.

The photo in the best quality available to us may be downloaded under www.kit.edu or requested by mail to presse@kit.edu or phone +49 721 608-21105. The photo may be used in the context given above exclusively.